Appendix 1.1

EXAMPLE OF RISK ASSESSMENT

As explained in Chapter 1, Bank Management must possess risk documentation, to allow risks that are identified and assessed or measured to be monitored by management; which is known as Risk Register. The creation of a risk register involves certain steps. There are currently various approaches, steps and methods that can be used in the assessment of risks in the use of Information Technology (IT), such as asset- or process-based approaches. The following is an example of **information security risk assessment** using an **asset-based approach**.

1. Document detailing results of Identification and Assessment of Risk (Risk Register)

Number	Asset	Risk Description	Susceptibility Analysis	Inherent			Existing Controls	Residual			Expected Final Risk Value
				Probability	Impact	Base Risk Value		Probability	Impact	Base Risk Value	
0	1	2	3	4	5	6	7	8	9	10	11

2. Risk Identification

2.1. Identification (Classification) of Assets

The first column, Asset, is filled by the name or type of assets created by a business process of the bank and assets which in turn support said business process. Here, assets are not limited to those from an accounting point of view, but everything with a value to the organization which must be secured, including data, software, hardware, communication and data networks, support facilities and human resources. Determine the owner of related assets and identify its critical importance to user and IT work units. For this identification process to work, Banks must first determine a certain assessment criteria to be used, for example:

Aspect	Sensitivity Analysis	Assessment Criteria		
		High	Medium	Low
Confidentiality	How large are the losses incurred by lost confidentiality of a piece of information?	If losses incurred are significant due to the sensitive nature of the information leaked or if the information is only accessible by certain personnel with specific authorization.	If losses incurred are not significant due to related information not being sensitive or accessible to various parties within the organization.	If losses incurred are very low due to related information being accessible to the public.
Integrity	How large is the effect/damage on business processes if an asset is used incorrectly, incomplete, inaccurate and out of date?	If effects caused are significant, such as the halting of business processes or potential of deviations with significant monetary value.	If effects caused are not significant, such as the halting of insignificant business processes or errors in decision making.	If effects caused are slight with no consequenc e on business processes.
Availability	How large is the effect/damage caused by the unavailability of an asset?	If effects caused are significant, such as the halting of business processes.	If effects caused are not significant due to related asset(s) being replaceable with acceptable loss of time and funds, thus only reducing efficiency and effectiveness of a business process.	If effects caused are very small, where related business processes are unaffected, or where related assets can be replaced promptly.

Assets classified according to sensitivity analysis and critical level establishment as shown in the table above are then inserted into the first column of the Risk Register form.

Example: Customer information in hardcopy

2.2. Identification and evaluation of risks related to assets

The second column of the Risk Register is filled with the results of identification and evaluation by users and IT personnel on the probability of failure or weaknesses in safeguarding procedures of defined assets as implemented by the Bank, which could cause significant effects on the Bank's performance. One asset may have more than one associated risk. Example of Column 2 (Risk Description): Information leaked to unauthorized parties.

2.3. Susceptibility Analysis

The third column of the Risk Register is filled with factors susceptible to failure or weaknesses of IT safeguarding as identified in the second column. Each risk can be associated with more than one susceptibility factor.
Example of Column 3:

- Safeguarding of archive/file storage cabinet is insufficient;
- Customer information is not kept where it is supposed to be.

3. Risk Assessment

The magnitude of impact of risks can be established by measuring its probability and consequence on business processes. Assessment criteria used refer to risk assessment methods used by the Bank. This process is carried out by personnel familiar with business processes ant information security on those processes. Columns 4, 5 and 6 are filled with the Bank's assessment results on probability and consequence of risks **before** controlling measures are applied on assets concerned with such risks. Meanwhile, columns 8, 9 and 10 are filled with results of the Bank's assessment on probability and consequence of risks **after** controlling measures are applied on assets concerned with such risks.

3.1. Probability Assessment

Column 4 of the Risk Register contains the **Inherent** Probability, which illustrates a risk's probability of occurring before controlling measures. Column 8 contains the **Residual** Probability, which illustrates a risk's probability of occurring after controlling measures. Probability may be assessed with assessment criteria, which is the quantitative value of the probability of a risk, as mentioned in its description, of occurring. The quantification of probability may take the form of the sum of occurrences in a given time unit, such as daily, weekly, monthly or annual.

Example of probability assessment criteria:

Level	Frequency of Occurrence	Probability of Occurrence
5	Extremely frequent	High short term probability
4	Frequent	High long term probability

Level	Frequency of Occurrence	Probability of Occurrence
3	Somewhat frequent	Medium probability
2	Rarely	Low probability
1	Almost never	Extremely low probability

Example of insertion of assessment result of Inherent Probability in column 4 of the Risk Register: ***Level 4***
Example of insertion of assessment result of Residual Probability in column 8 of the Risk Register: ***Level 3***

3.2. Impact Assessment

Column 5 of the Risk Register contains the **Inherent** Impact which illustrates the severity of damage caused by the occurrence of a risk relative to an asset before controlling measures are in place. Column 9 of the Risk Register contains the **Residual** Impact which illustrates the severity of damage caused by the occurrence of a risk relative to an asset after controlling measures are in place.

Example of impact classification:

Score	Probability of disturbance on Business Processes	Probability of decline in Reputation
5	Information Processing Assets experiences total failure causing entirety of the bank's business being disrupted.	Reputation damage resulting in serious and continuous decline of reputation in the eyes of customers, primary stakeholders, the financial market and the general public, both global and regional.
4	Information Processing Assets experiences disturbances causing disruption on the bank's business activities until related Information Processing Assets are restored.	Partial reputation damage – only for particular customers or counterparties.
3	Information Processing Assets experiences disturbances causing disruption on some of the bank's business activities until related Information	Partial reputation damage – only on some divisions/sections/teams.

Score	Probability of disturbance on Business Processes	Probability of decline in Reputation
	Processing Assets are restored.	
2	Information Processing Assets experiences disturbances, but main duty activities of related Teams can be carried out in a normal fashion due to said information processing assets being replaceable by other Information Processing Assets.	Partial reputation damage – only on certain work units.
1	No disturbance of any kind on business process operations.	No impact on reputation.

Example of insertion of impact assessment result in column 5 of the Risk Register: ***Level 5***
Example of insertion of impact assessment result in column 9 of the Risk Register: ***Level 2***

3.3. Establishment of Risk Value

Column 6 of the Risk Register contains the **Base Risk Value (BRV)** which constitutes an asset's risk level **before** controlling measures are in place. Column 10 of the Risk Register contains the **Final Risk Value (FRV)** which constitutes an asset's risk level **after** controlling measures are in place. As previously explained in Chapter 1, Banks can devise their own grading methods through a risk assessment matrix. Risk assessment in the following example uses 3 levels/grades, which are Low, Medium and High:

Trend						
	5	*Medium*	*Medium*	*High*	*High*	*High*
	4	*Low*	*Medium*	*High*	*High*	*High*
	3	*Low*	*Low*	*Medium*	*High*	*High*
	2	*Low*	*Low*	*Medium*	*Medium*	*High*
	1	*Low*	*Low*	*Medium*	*Medium*	*High*
		1	2	3	4	5
				Impact		

Example of insertion of BRV establishment in column 6: ***High***
Example of insertion of FRV establishment in column 10: ***Medium***

4. Identification of Implemented Control Measures

Column 7 of the Risk Register contains control measures which have been implemented by the Bank to mitigate the risks on identified assets, such as:

- policies and procedures related to said asset;
- the use of certain technologies for risk control, either automatically, or by system-control, such as audit logs, on line approval and the system's parameter values.

Example of control measures inserted into column 7 for assets in the form of hardcopies of customer information:

- archiving regulations;
- PIN-based access-restriction for the archive room;
- use of CCTVs.

5. Expected Risk Value

Banks should establish an expected risk value (risk limit) on all identified risks. For example, if the risk of customer information being compromised is expected to be low, then Low is inserted into column 11.

6. Risk Value Analysis

The following is an example of how to fill the Risk Register Form after following the steps above:

Asset	Risk Description	Susceptibility Analysis	Inherent			Existing Controls	Residual			Expected Risk Value
			Probability (min = 1, max = 5)	Impact (min = 1, max = 5)	Base Risk Value		Probability (min = 1, max = 5)	Impact (min = 1, max = 5)	Final Risk Value	
1	2	3	4	5	6	7	8	9	10	11
Hardcopies of customer information	Information is leaked to unauthorized parties	Archive storage cabinets are insufficiently secured	Level 4	Level 5	HIGH	- Archiving regulations - PIN based access restriction for the archive room - use of CCTVs	Level 3	Level 2	MEDIUM	LOW
		Customer information documents are misplaced								

After the Risk Register form is filled, the Bank conducts a risk value analysis on each identified asset. The difference between a High BRV and a Medium FRV illustrates how decline in a risk's probability of occurrence and impact severity will not be as significant without the proper implementation of a risk control system. Banks should analyze the possibility of implementing control measures for risks not previously covered. Comparison between the FRV and the Expected Risk Value on various identified assets is the base parameter to mitigate risks. For example, if the expected risk level for leakage of customer information is LOW, while its FRV is still MEDIUM, additional control measures must be taken. Subsequently, Banks must establish a Risk Control Plan for related assets. For instance, the Bank needs to enhance its risk control system for information security, and to update its policies and procedures on security.